DEPARTMENT OF NATIONAL DEFENCE
CANADA

OPERATIONAL RESEARCH DIVISION

DIRECTORATE OF OPERATIONAL RESEARCH (JOINT & LAND)

DOR(J&L) RESEARCH NOTE RN 9802

ASSESSMENT OF JOINT WARRIOR INTEROPERABILITY DEMONSTRATION (JWID) 97 NETWORK LATENCY INDUCED BY THE SAGUS SECURITY GATEWAY

By

Dr. P. O'Neill

FEBRUARY 1998

OTTAWA, CANADA

National Defence Défense nationale

102-02391/

OPERATIONAL RESEARCH DIVISION

CATEGORIES OF PUBLICATION

ORD Reports are the most authoritative and most carefully considered publications of the DGOR scientific community. They normally embody the results of major research activities or are significant works of lasting value or provide a comprehensive view on major defence research initiatives. ORD Reports are approved personally by DGOR, and are subject to peer review.

ORD Project Reports record the analysis and results of studies conducted for specific sponsors. This Category is the main vehicle to report completed research to the sponsors and may also describe a significant milestone in ongoing work. They are approved by DGOR and are subject to peer review. They are released initially to sponsors and may, with sponsor approval, be released to other agencies having an interest in the material.

Directorate Research Notes are issued by directorates. They are intended to outline, develop or document proposals, ideas, analysis or models which do not warrant more formal publication. They may record development work done in support of sponsored projects which could be applied elsewhere in the future. As such they help serve as the corporate scientific memory of the directorates.

ORD Journal Reprints provide readily available copies of articles published with DGOR approval, by OR researchers in learned journals, open technical publications, proceedings, etc.

ORD Contractor Reports document research done under contract of DGOR agencies by industrial concerns, universities, consultants, other government departments or agencies, etc. The scientific content is the responsibility of the originator but has been reviewed by the scientific authority for the contract and approved for release by DGOR.

DEPARTMENT OF NATIONAL DEFENCE

CANADA

OPERATIONAL RESEARCH DIVISION

DIRECTORATE OF OPERATIONAL RESEARCH (JOINT & LAND)

DOR(J&L) RESEARCH NOTE RN 9802

ASSESSMENT OF JOINT WARRIOR INTEROPERABILITY DEMONSTRATION (JWID) 97 NETWORK LATENCY INDUCED BY THE SAGUS SECURITY GATEWAY

by

Dr. P. O'Neill

Recommended by: _____
R.E. Kluchert
JSORT

Approved by: _____
G. Lafond
DOR(J&L)

Directorate Research Notes are written to document material which does not warrant or require more formal publication. The contents do not necessarily reflect the views of ORD or the Canadian Department of National Defence.

OTTAWA, ONTARIO

FEBRUARY 1998

ABSTRACT

This note describes a procedure for measuring the latency induced in the Joint Warrior Interoperability Demonstration (JWID) 97 network by the Sagus Corp. Security Gateway. Tests carried out during JWID 97 indicate that no additional latency results from the gateway. The basic testing approach is described along with the attendant statistical test of significance, which is based on a randomization test.

TABLE OF CONTENTS

PAGE

ABSTRACT i
TABLE OF CONTENTS ii
INTRODUCTION 1
BACKGROUND 1
NATIONAL OBJECTIVES 4
THE TEST PROCEDURE 5
THE TEST RESULTS 6
CONCLUSIONS 8
REFERENCES 9

ASSESSMENT OF JOINT WARRIOR INTEROPERABILITY DEMONSTRATION (JWID) 97 NETWORK LATENCY INDUCED BY THE SAGUS SECURITY GATEWAY

INTRODUCTION

1. This note describes a test procedure used during Joint Warrior Interoperability Demonstration (JWID) 97 to determine whether or not the Sagus Corporation security gateway introduced any significant delay in the transmission of data through the coalition network. The procedure was designed and implemented to address the concern of various staffs of the Director General Information Management that the data processing speed of the gateway might create a "bottleneck".

2. Further to discussions at Reference 1, the author designed a test of latency. The design and conduct of the test were ultimately accomplished with the assistance of Mr. Marcel Deveaux of Sagus Corp who served as subject matter expert on both the Sagus software and the JWID 97 network configuration.

3. Analyses of the test results indicate that with 92% assurance, the Sagus gateway does not impede the average network response time.

4. The remainder of the report is organised as follows. Some background information, drawn from Reference 2, describes the JWID 97 coalition network and the potential latency problem. Following this, the test procedure is described along with the test results. The conclusions drawn from analysis of the test results complete the report.

BACKGROUND

5. Currently the Command and Control (C^2) and Intelligence communities operate on separate platforms and infrastructures with varying levels of integration and interoperability. Information transfer between the various systems is challenging at best and usually requires manual intervention. The current departmental direction and vision of

an Integrated Information Environment (IIE) and Common User Core (CUC) is an attempt to increase the ability of information systems to share information. JWIDs provide a forum to test functionality and interoperability in a joint and combined environment, to gain an awareness of new technological solutions to chronic Command and Control Information System (CCIS) problems, and to evolve operational doctrine to maximise the impact of technology on operational effectiveness.

6. The participation in JWID 97 was a co-operative effort spanning international borders, strategic and operational systems, and multiple capital projects. This effort involved engineering teams from AUSCANNZUKUS, from NDHQ and the commands, and from the CCIS projects. This year's participation was primarily restricted to the use of fielded CCIS systems such as the Joint Command and Control Information System (JC2IS) in order to assess interoperability and functionality weaknesses and to provide direction to the CCIS projects' definition activities. A primary technical objective was to prove elements of a proposed security architecture, which included network encryption using Motorola Network Encryption System (NES) and guard technology using the Sagus Defensor Gateway.

7. Canadian elements were deployed in two caveat domains classified SECRET: a Coalition Wide Area Network (CWAN) and a notional Canadian Eyes Only Wide Area Network (CEO WAN). Tunnelling on the Defence Wide Area Network (DWAN) using Motorola NES created the notional CEO WAN. The CWAN and the CEO WAN were interconnected only through, the Sagus Defensor Gateway.

8. Figure 1 depicts the following elements, which were deployed on the CWAN and CEO WAN:

a. A deployed Joint Forces Headquarters (JFHQ) acted as a National Command Element (NCE) in Suffolk, Virginia. It resided on the CWAN and used JC2IS as its primary CCIS;

b. A SimNDOC was established in the JSAT Conference Room at NDHQ. It resided on the CEO WAN and used JC2IS as its primary CCIS. J2 Geo provided a geomatics services demonstration. The Sagus Defensor Guard resided in the SimNDOC as well, demonstrating its functionality across the CWAN and CEO WAN;

c. An Air Operations Centre (AOC) was established in Winnipeg. It resided on the CEO WAN and was connected to Wing Operations Centres (WOCs) in Cold Lake and Comox; and

d. A Maritime Operations Centre (MOC) was established in Esquimalt. It resided on the CEO WAN and used JMCIS as primary CCIS. A simulated frigate resided on the CWAN as part of the Multi-national Naval Task Group (MNTG).

9. Information was exchanged and shared among participants using various mechanisms: SMTP mail (email), FTP (file transfer), Telenet (terminal sessions), HTTP (world-wide web), structured messages (X.400, OTH Gold etc.), and database replication mechanisms.

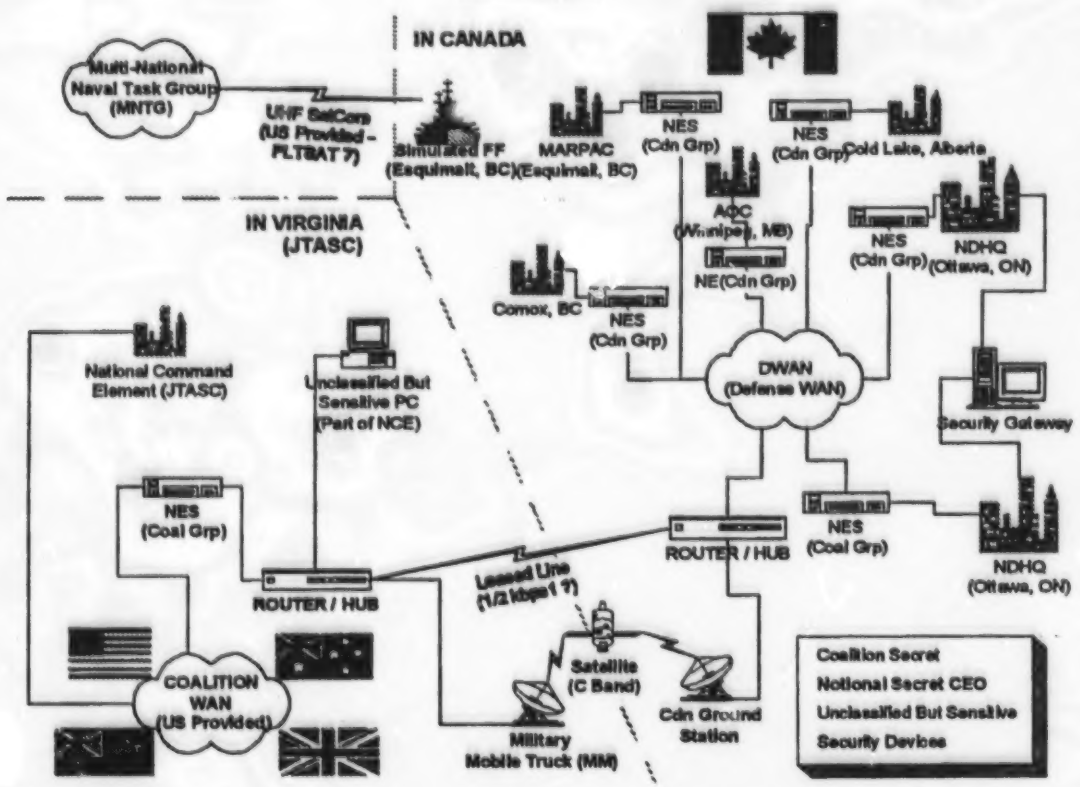

Figure 1: Coalition Network for JWID 97

NATIONAL OBJECTIVES

10. The main Canadian aim for JWID 97 was to evaluate the capabilities of current Canadian Command and Control Information Systems by providing interoperability with coalition partners while exposing operations personnel, technical and project teams to the latest CCIS technology innovations demonstrated in JWID 97. Specifically, the following national objectives had been set:

a. Simulate the deployment of a Canadian Joint Force Headquarters (JFHQ) to a coalition site with the intent to test and evaluate Canadian C2IS in life-like scenarios;

b. Exercise the Operational Planning Process through the different phases of the operation involving a Canadian Joint Force as part of the coalition;

c. To further the development of joint and combined command and control doctrine to help resolve interoperability issues;

d. To progress the practical examination of the US Global Command and Control System (GCCS) and the US Global Command Support Systems (GCSS) as the Canadian Forces migrates its command and control systems to be compliant and interoperable with the US Common Operating environment;

e. To demonstrate enhanced exchange to joint/combined forces and improved C3 effectiveness and interoperability through the extension of IP based networking at sea;

f. Assess Security tunnelling through the Defence Wide Area Network (DWAN);

g. Evaluate the state of technology in security firewalls and possible security policy issues for the Canadian Forces;

h. Assess the success of implementation of the Coalition Network; and

j. Demonstrate the sharing of geospatial data files between Canadian and Coalition forces, including geospatial database updates requiring collaborative co-production, and the ability to import, display and manipulate these files in GCCS-CHART or its replacement.

THE TEST PROCEDURE

11. Prior to the start of the exercise, in discussions at Reference 2, it was proposed that a simple mechanism like SMTP mail, the File Transfer Protocol (FTP) or the UNIX "ping" command should be used to measure latency induced by the coalition security gateway.

12. After discussing the requirements and the available practical options with Mr Deveaux, during JWID 97, it was decided that the FTP command would be the most appropriate means of testing latency. The main reason that FTP was chosen over SMTP is that SMTP "spools" data transfers and therefore the elapsed times reported by SMTP are not direct measures of the elapsed time for the actual data transfer itself. The "ping" command was deemed unsuitable because it was determined that "pinging" across the gateway was impossible.

13. During JWID 97 some difficulty had been experienced with the gateway because of the use of non-approved file formats by participants in the demonstration. Prior to the beginning of the demonstration it had been stressed that only files that satisfied pre-approved formats and security conventions could be transferred across the gateway. Initially this had resulted in some file transfers being blocked. However, once such matters had been cleared up, the speed of the gateway could be tested.

14. After a few trials of the FTP command, it was determined that a viable test of latency introduced by the JWID coalition gateway could be accomplished as follows:

- FTP could be used to "get" and "put" a reference text file (412KB ASCII) between SIM NDOC (Ottawa) and SIM JFHQ (Suffolk, VA) using two routes: a Canadian-Eyes-Only route (denoted by "CEO") that would not pass through the gateway; and a coalition route (denoted by "COALITION") that would pass through the gateway.

15. The alternative routes are shown in Figure 2. The CEO route uses nodes 1, 2, 6, 7... 11. The COALITION route uses nodes 1, 3, 4, 5, 6, 7... 11. The Sagus security gateway is node 3.

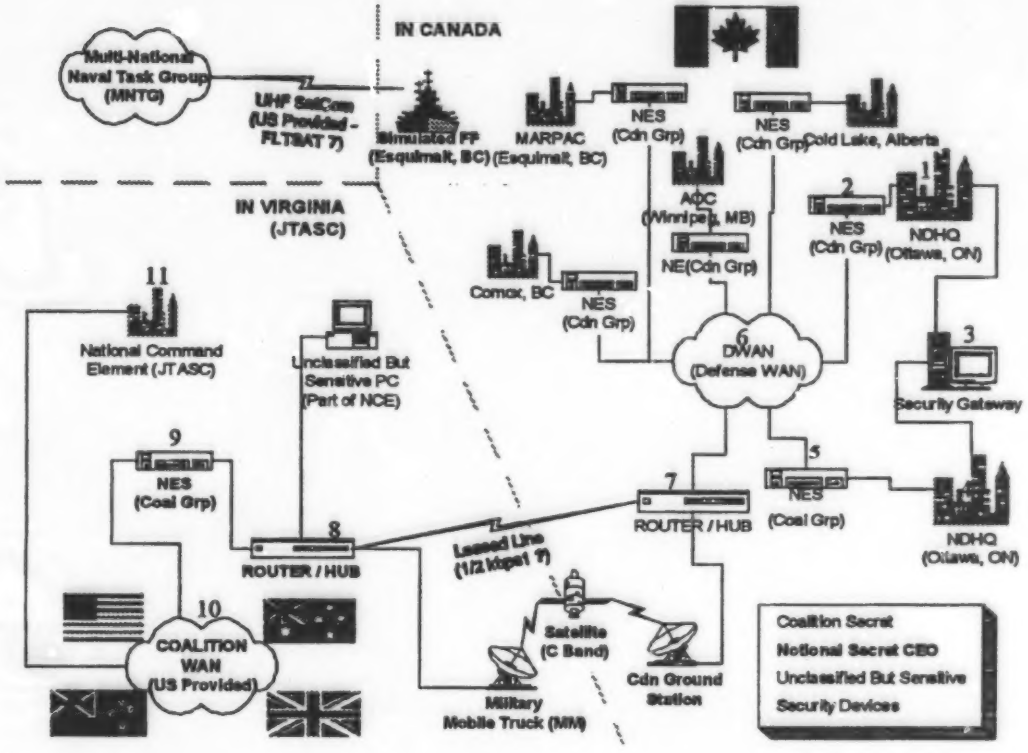

Figure 2: Alternative Routes for FTP Test with Sagus Gateway at Node 3.

THE TEST RESULTS

16. On 28 July, between 1600 and 1630, a period of moderate activity on the network, Mr Deveaux executed 12 file transfers as outlined in the previous paragraph. The elapsed times reported by the system in seconds for each transfer are given in Table 1.

TABLE I
FTP REPORTED ELAPSED TIMINGS (SECONDS)

28 July1600-1630		FTP 412KB ASCII	
	trial	CEO	COALITION
	1	31	32
GET	2	31	31
	3	31	29
	4	31	27
PUT	5	29	27
	6	29	27

17. Average timings are shown in Table 2.

TABLE II
FTP AVERAGE ELAPSED TIMINGS (SECONDS)

	CEO	COALITION
GET	31	30.67
PUT	29.67	27

18. At first glance, it appears that the "put" operation executes faster than the "get" operation and that the "COALITION" route is faster than the "CEO" route. Note, however, that the sample size for each treatment of the data is somewhat small (6 trials).

19. Statistical significance of the hypotheses were tested using randomisation tests (Reference 3):

- The hypothesis *"put" is faster than "get"* was tested by estimating the proportion of samples of size 6 drawn at random from the total population of 12 that have an average elapsed time greater than 28.33 (the observed average for all 6 of the "put" operations). It was found that with probability >0.99, "put" is faster than "get".

- The hypothesis *"COALITION" route is faster than "CEO" route* was tested by estimating the proportion of samples of size 6 drawn at random from the total population of 12 that have an average elapsed time greater than 28.83 (the observed average for all 6 of the "COALITION" route

transfers). It was found that with probability >0.92, the "COALITION" route is faster than the "CEO" route.

CONCLUSION

20. The data suggests that the coalition gateway introduced no additional latency into the network response time. In other words, the processing speeds of other components of the network were the driving factors of latency during JWID 97.

REFERENCES

1. Meeting Maj. Tim Pascal, DDCEI 2-4 / Dr Phil O'Neill, JSORT 2, 5 June 1997

2. 3000-14(J3 Plans & Ops 4-4) June 1997, JWID 97 - Canadian Operational Order

3. Edgington, Eugene S., "Randomization Tests", Marcel Dekker Inc., New York, 1980.

UNCLASSIFIED

SECURITY CLASSIFICATION OF FORM
(highest classification of Title, Abstract, Keywords)

DOCUMENT CONTROL DATA
(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (the name and address of the organization preparing the document. Organizations for whom the document was prepared e.g. Establishment Sponsoring a contractor's report, or tasking agency, are entered in Section 8).

Operational Research Division
Department of National Defence
Ottawa, Ontario K1A 0K2

2. SECURITY CLASSIFICATION (overall security classification of the document, including special warning terms if applicable)

UNCLASSIFIED

3. TITLE (the complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title)

Assessment of Joint Warrior Interoperability Demonstration (JWID) 97 Network Latency Induced by the SAGUS Security Gateway

4. AUTHORS (last name, first name, middle initial)

O'Neill, Dr. P.

5. DATE OF PUBLICATION (month Year of Publication of document)	6a. NO OF PAGES (total containing information. Include Annexes, Appendices, etc.)	6b. NO OF REFS (total cited in document)
February 1998	14	3

7. DESCRIPTIVE NOTES (the category of document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Research Note

8. SPONSORING ACTIVITY (the name of the department project office or laboratory sponsoring the research and development. Include the address).

J3 Doc & Trg

9a. PROJECT OR GRANT NO. (if appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (if appropriate, the applicable number under which the document was written.)
3551-20209	---

10a. ORIGINATOR's document number (the official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NOS. (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DOR(J&L) Research Note RN 9801	---

11. DOCUMENT AVAILABILITY (any limitations on further dissemination of the document, other than those imposed by security classification.)

(X) Unlimited distribution
( ) Distribution limited to defence departments and defence contractors: further distribution only as approved
( ) Distribution limited to defence departments and Canadian defence contractors; further distribution only as approved
( ) Distribution limited to government departments and agencies; further distribution only as approved
( ) Distribution limited to defence departments; further distribution only as approved
( ) Other (please specify):

12. DOCUMENT ANNOUNCEMENT (any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in 11) is possible, a wider announcement audience may be selected.)

13. ABSTRACT (a brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual).

This note describes a procedure for measuring the latency induced in the Joint Warrior Interoperability Demonstration (JWID) 97 network by the Sagus Corp. Security Gateway. Tests carried out during JWID 97 indicate that no additional latency results from the gateway. The basic testing approach is described along with the attendant statistical test of significance, which is based on a randomization test.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus-identified . If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Network latency
Network security
Design of testing